UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/590,794 | 09/18/2006 | **Marc Girault** | P1924US | 2203 |

8968 7590 04/02/2009

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

| EXAMINER | |
|---|---|
| VAUGHAN, MICHAEL R | |
| **ART UNIT** | **PAPER NUMBER** |
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 04/02/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/590,794 | GIRAULT ET AL. | |
| | Examiner | Art Unit | |
| | MICHAEL R. VAUGHAN | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *09 February 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

The instant application having Application No. 10/590,794 is presented for examination by the examiner. Claims 1, 5, 6, 9, 10, 11, 13, 14, 17, 19, 21, and 22 have been amended. Claims 1-23 are pending.

## *Response to Amendment*

### *Claim Objections*

The currently filed amendment overcomes the previous claim objections.

### *Claim Rejections - 35 USC § 101*

The current amendment overcomes the previous 101 claim rejections.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claims are generally narrative and indefinite, failing to conform to current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors. Examiner advises Applicant to carefully craft the claim language so that it is precise and clearly sets forth the metes and bounds of the claim. Examiner made this suggestion in the previous Action and some of the deficiencies were corrected. However many more exist which render the claims indefinite and hard to understand.

For example in claim 1, the phrase in the preamble, "including a part at least of a secret key" is indefinite. Clearly this must be some mistranslation of the foreign application. It is still unclear how the secret key relates to the first and second factors.

What does "in the absence of any completed effective multiplication operation" mean? This is from the same limitation which states that a multiplication operation is carried out. The preamble also states at least one multiplication operation is performed between two factors. The claim seems to contradict itself as to if and where a multiplication operation is performed.

Besides grammatically deficiencies, indefiniteness is found by the lack of distinct limitations. For example in claim 1, the preamble says that a cryptographic value (y) is produced; however nowhere in the body of the claim is it explicit that the value is produced. The first limitation recites a binary representation. The second limitation then redefines a binary representation. Are they the same? Do the first factor and the second factor share the same binary representation? The claims do not distinctly point this out. It is unclear what is implied by the verb selecting. Is this function necessary

and if so what constitutes selecting a factor? Examiner likens it to the function of reading because it is followed by memorizing. So it seems the factor is read perhaps from memory (not claimed) and stored in another memory such as a register. This is a narrow interpretation just to try and make sense of it. Clearly there is no memory or register present in the claim. Independent claim 17 shares many of the same problems as claim 1. The dependent claims do not overcome these problems as well.

From these deficiencies, it is unclear to the Examiner what exactly is being performed in the claim. The claim seems to be directed to multiplying two factors but the process and result is mired beneath indefiniteness and ambiguities. Examiner still cannot ascertain the scope of the invention due to these aforementioned problems. Examiner will still however, examine the claims given the broadest interpretation in light of these 35 USC 112 second paragraph problems and the specification.

## *Response to Arguments*

Applicant's arguments filed 2/09/09 have been fully considered but they are not persuasive. Examiner has attempted to understand the claims in light of all of the aforementioned problems and understanding thereof. Examiner was hoping the previous rejections and suggestions would help Applicant amend the claims to put them in better form for prosecution. However, the amendments do not rectify or clear up the indefiniteness of the claims. Therefore it is still impossible to ascertain the scope of the invention. It appears the independent claims are directed to multiplying two factors by first formatting one or both of them with padding bits. Once the two factors are properly

formatting, multiplication can be performed through some mysterious shifting and assembling. Examiner also had hoped that the Applicant's remarks would shed light the differences between the amended claimed invention and the cited prior art. However, the majority of the remarks were directed to questioning how Examiner has interpreted the prior art. Applicant states that the Naslund references could only be done a processor and hence is different from the claimed invention, yet amended the claims to add a processor.

Given Examiner's aforementioned interpretation of the independent claims, Examiner finds Naslund to teach these limitations. The first and second factors correspond to the alpha and beta factor of paragraph 0131. Naslund teaches performing many types of operations (including multiplication, 0131 & 0166) on these two factors (0089). What is key to his invention are the guard bits. In order to reduce the complexity of the operations, single or multiple guards bits are positions between the bits of the factors. Then, depending of the operations, various functions are performed on the bits, such as shifting and other logical functions to carry out the mathematics. Naslund stores the first factor in a first field and the second factor is a second field. Then the product is stored in a third field (0089).

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-23 are rejected under 35 U.S.C. 102(e) as being anticipated by USP Application Publication 2006/0072743 to Naslund et al., hereinafter Naslund.

As per claims 1 and 17, Naslund teaches a method and device for performing a cryptographic operation in a device under the control of a security application, in which a cryptographic value (y) is produced in the device, by a calculation comprising at least one multiplication between a first and a second factor [alpha, beta] including a part at least of a secret key (s) associated with the device (0131),

wherein the first of the two factors of the multiplication has a determined number of bits L in binary representation (0132),

the second of the two factors comprises, in binary representation, having several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L - 1 bits set to 0 [multiple-guard bits; 0087],

selecting and memorizing successive binary versions of the first factor by shifting said first factor in accordance with the positions of the bits set to 1 of the second factor (shifting done in 0089);

carrying out the multiplication operation by assembling successive shifted versions of the selected and memorized shifted binary versions of the first factor,

thereby allowing said cryptographic operation to be conducted in the absence of any completed effective multiplication operation due to said shifting and assembling [multiplication is performed by the shifting and result in the product equal to the third field element; 0089] .

As per claim 2, Naslund teaches the secret key (s) forms part of an asymmetric cryptographic key pair associated with the device (0274).

As per claim 3, Naslund teaches the device comprises a chip including hard-wired logic for producing the cryptographic value (0063).

As per claim 4, Naslund teaches the calculation of the cryptographic value furthermore comprises an addition or a subtraction between a pseudo-random number and the result of the multiplication (0275 and 0306).

As per claim 5, Naslund teaches the first and second factors and the pseudo-random number are dimensioned so that the pseudo-random number is greater than the result of the multiplication (0312).

As per claim 6, Naslund teaches the number of bits set to 1 of the second factor is chosen at most equal to the largest integer less than or equal to s1/L, where s1 is a predefined threshold less than the number of bits of the pseudo-random number (r) in binary representation (0168).

As per claim 7, Naslund teaches the two factors of the multiplication include, as well as said part of the secret key, a number provided to the device by the security application executed outside the device (0274).

As per claim 8, Naslund teaches the two factors of the multiplication include, as well as said secret key, a number provided by the device (0274).

As per claim 9, Naslund teaches part of the secret key (s) is said first factor of the multiplication (0275).

As per claim 10, Naslund teaches binary versions are disposed in respective intervals of like size in bits, said size corresponding to the total size of a usable space, divided by the number of bits set to 1 of the second factor of the multiplication, each binary version being placed in its respective interval as a function of a shift in accordance with the positions of the bits set to 1 of the second factor (0168).

As per claim 11, Naslund teaches part of the secret key (s) is the second factor of the multiplication (0276).

As per claim 12, Naslund teaches the secret key is stored in a memory support of the device by coding the positions of its bits set to 1 (0276).

As per claim 13, Naslund teaches the secret key (s) is stored in a memory support (-1-6) of the device by coding numbers of bits separating respectively lower bounds of intervals of (S- 1)/(n- 1) bits and lower bounds of blocks of bits allotted to the first factor (c) of the multiplication and each disposed in the associated intervals, S being the number of bits of the secret key and n the number of bits set to 1 of the secret key (0168 and 0276).

As per claim 14, Naslund teaches the secret key is stored in a memory support of the device by coding numbers of bits, each representative of the number of bits

separating two blocks of successive bits allotted to the first factor of the multiplication (0276).

As per claim 15, Naslund teaches the cryptographic value is produced so as to authenticate the device in a transaction with the security application executed outside the device (0304).

As per claim 16, Naslund teaches the cryptographic value is produced in the guise of electronic signature (0014).

As per claim 18, Naslund teaches generating a pseudo-random number (r), the means of calculation comprising means for adding the result of the multiplication to or subtracting it from said pseudo- random number (0275 and 0306).

As per claim 19, Naslund teaches the first and second factors and the pseudo-random number are dimensioned so that the pseudo-random number is greater than the result of the multiplication (0312).

As per claim 20, Naslund teaches the means of calculation are embodied as hard-wired logic (0063).

As per claim 21, Naslund teaches part of the secret key is the first factor of the multiplication (0275).

As per claim 22, Naslund teaches part of the secret key (s) is the second factor of the multiplication (0276).

As per claim 23, Naslund teaches a memory adapted for storing data for coding the positions of the bits set to 1 of the secret key (0276).

## *Conclusion*

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431